National Infrastructure Protection Center
CyberNotes

Issue #2001-08 April 23, 2001

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between April 5 and April 20, 2001. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alcatel[1]	Multiple	Speed Touch Home KHDSAA 108, 132, 133, 134	Several vulnerabilities exist which are the result of weak authentication and access control policies that could let a remote malicious user gain unauthorized access, sensitive information, cause a Denial of Service, and make changes to configuration and firmware.	Please see advisory located at: http://www.alcatel.com/consumer/dsl/security.htm	Multiple Speed Touch ADSL Insecure Administration Interface	**High**	Bug discussed in newsgroups and websites.

[1] CERT® Advisory CA-2001-08, April 11, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
AnalogX[2]	Windows 98/98/ME/ NT 4.0	Simple Server: WWW 1.0.3- 1.0.8	A remote Denial of Service vulnerability exists when an HTTP GET is requested from the /aux directory.	Upgrade available at: http://www.analogx.com/files/sswwwi.exe	SimpleServer WWW /aux Directory Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
BinTec[3]	Multiple	BinTec X1200 5.1, X4000 5.1.6 patch 10, 5.3 Rev 1	A remote Denial of Service vulnerability exists when the router receives a connection on port 1723/TCP (PPTP Service) or port 53/UDP, and has not had the registration key entered into the router firmware.	**Temporary workaround:** Create an access control entry denying connections to port 1723/TCP.	BinTec X Series Router PPTP Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco Systems[4]	Multiple	PIX Firewall 5.1.4	A Denial of Service vulnerability exists when multiple requests for TACACS+ authentication are received.	Upgrade available at: http://www.cisco.com/public/support/tac/home.shtml	PIX TACACS+ Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco Systems[5]	Multiple	VPN 3000 Concentrator 2.5.2(A), 2.5.2(B), 2.5.2(C), 2.5.2(D)	A remote Denial of Service vulnerability exists when a specially crafted IP packet is sent with an invalid IP option setting.	Upgrade available at: http://www.cisco.com/public/sw-center/	VPN 3000 Concentrator Malformed IP Packet	Low	Bug discussed in newsgroups and websites.
Cisco Systems[6]	Multiple	Catalyst models 5000, 5002, 5500, 5505, 5509; 2901, 2902 and 2926 switches	A remote Denial of Service vulnerability exists when an 802.1x frame is sent to a switch that has the spanning tree protocol blocked.	Upgrade available at: http://www.cisco.com	Catalyst 802.1x Frame Forwarding	Low	Bug discussed in newsgroups and websites.
CrossWind[7]	Windows NT 2000, Unix	Cyber Scheduler 2.1	A buffer overflow vulnerability exists in the daemon 'websyncd' timezone string parser, which could let a remote malicious user execute arbitrary code as root.	Patch available at: http://www.crosswind.com/cybdata.htm	Cyber Scheduler 'websyncd' Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Darren Hiebert[8]	Unix	Ctags 1.0-3.2.3	A vulnerability exists due to an insecure use of temporary files, which could let a malicious user overwrite the contents of the target file with its own output.	Update available at: http://security.debian.org/dists/stable/updates/main	Ctags Symbolic Link Attack	Medium	Bug discussed in newsgroups and websites.

[2] Securiteam, April 18, 2001.
[3] Securiteam, April 9, 2001.
[4] Securiteam, April 12, 2001.
[5] Cisco Security Advisory, CI-04.05, April 12, 2001.
[6] Cisco Security Advisory, April 16, 2001.
[7] Defcom Labs Advisory, def-2000-18, April 17, 2001.
[8] Debian Security Advisory, DSA-046-2, April 19, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DC Scripts[9]	Multiple	DCForum 2000 1.0	A vulnerability exists due to the failure to properly validate user-supplied input to the script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	DCForum 'AZ' Field Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
Francisco Burzi[10]	Multiple	PHP-Nuke 1.0, 2.5, 3.0, 4.0, 4.3, 4.4	A vulnerability exists which could let a remote malicious user submit a query string to the server specifying a new destination URL be opened when clicking on the site's ad banners.	Update available at: http://phpnuke.org/download.php?dcategory=Fixes	PHP Nuke Remote Ad Banner URL Change	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Fujitsu-Siemens[11]	Unix	Siemens Reliant UNIT 5.43, 5.44, 5.45	A vulnerability exists due to the improper checking of file creation rights by the ppd software package, which could let a malicious user overwrite sensitive system files, potentially denying service to legitimate users, and possibly gaining elevated privileges.	No workaround or patch available at time of publishing.	Reliant Unix ppd -t Race Condition	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
GoAhead Software[12]	Windows 98/ME	GoAhead Webserver (Windows) 2.1	A remote Denial of Service vulnerability exists when a request is made to the /aux directory.	No workaround or patch available at time of publishing.	GoAhead Webserver /aux Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Hylafax[13]	Multiple	Hylafax 4.0pl0, 4.0pl1, 4.0pl2, 4.1-beta1, beta2, beta3	A format string vulnerability exists in the server binary 'hfaxd', which could let a malicious user execute arbitrary code.	Patch available at: http://www.hylafax.org/patches/hfaxd-vulnerability.patch	Hylafax 'hfaxd' Local Format String	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[14]	Windows NT 4.0, Unix	Net Commerce 3.1.2	Two remote vulnerabilities exist: a Denial of Service due to the way long strings are handled by the macro.d2w CGI; and by directly referencing the macro.d2w file with an extension of NOEXISTINGHTMLBLOCK, a remote malicious user could gain sensitive information.	No workaround or patch available at time of publishing.	Websphere/ Net.Commerce CGI-BIN Macro Denial of Service and Installation Directory Revealing	Low/ Medium	Bug discussed in newsgroups and websites. Exploits have been published.
Imatix[15]	Windows 98/ME	Xitami for Windows 2.4d7, 2.5d4	A remote Denial of Service vulnerability exists when an URL request for an MS-DOS device name is submitted.	The vendor plans to release a minor update with a work around for this issue. This update will be announced on the Xitami user mailing list and announcement list when it is available.	Xitami Webserver MS-DOS Device Name Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[9] qDefense Advisory Number QDAV-5-2000-1, April 16, 2001.
[10] Bugtraq, April 4, 2001.
[11] Securiteam, April 10, 2001.
[12] Bugtraq, April 17, 2001.
[13] Securiteam, April 12, 2001.
[14] Bugtraq, April 13, 2001.
[15] Bugtraq, April 17, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Infopop Corporation[16]	Unix	Ultimate Bulletin Board 5.43, 5.4.7e	A vulnerability exists when modified URLs are submitted, which could let a remote malicious user bypass forum membership restrictions and password requirements to read arbitrary messages.	Upgrade available at: http://www.infopop.com/business/business_ubb.html	Ultimate Bulletin Board Forum Password Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
iPlanet[17]	Windows NT 4.0, Unix	Calendar Server 2.1-2.1p3, 5.0p1- 5.0p2	A vulnerability exists due to inadequate security settings for the configuration files, which could allow a malicious user to gain access to the cleartext version of a valid username and password.	No workaround or patch available at time of publishing.	Calendar Server Plaintext Admin Password	Medium	Bug discussed in newsgroups and websites.
Lightwave[18]	Multiple	Console Server 3200	Two vulnerabilities exist: a brute force style password vulnerability; and the unit's remote administration interface supplies sensitive information to users who have not successfully logged into an administrative account.	**Workaround:** VPNs are the norm for the 3200. The ConsoleServer 3200 (at the moment) does not support SSH, SSL, Secure ID, or any other authentication and should (in security-sensitive applications) be deployed behind the firewall. An upgrade will be available this summer.	ConsoleServer Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Lotus[19]	Windows NT 4.0/2000, Unix, OS/2 4.5Warp, OS/390 V2R9	Lotus Domino 5.0.1-5.0.6	Multiple Denial of Service vulnerabilities exist: due to the handling of unusual input in various HTTP headers; a remotely submitted GET request composed of an arbitrary string of Unicode characters; a large number of requests made to access DOS-devices through the web server; a continuos stream of connects with a payload of 10K data followed by return to TCP port 63148 (DIIOP - CORBA); and large HTTP requests made to TCP port 80.	Upgrade available at: http://www.notes.net/qmrdown.nsf/QMRWelcome	Lotus Domino Server Multiple Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites.
Matt Tourtillott[20]	Unix	Nph-maillist 3.0, 3.5	A vulnerability exists in the CGI script, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Nph-maillist Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[16] Bugtraq, April 5, 2001.
[17] Securiteam, April 20, 2001.
[18] Securiteam, April 11, 2001.
[19] Defcom Labs Advisory def-2001-20, April 11, 2001.
[20] Bugtraq, April 10, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[21]	Windows 2000	ISA Server 2000	A Denial of Service vulnerability exists if a HTTP request with an unusually long path is submitted,	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-021.asp	Windows 2000 Internet & Acceleration Server Denial of Service CVE Name: CAN-2001-0239	Low	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the Press and other public media.
Microsoft[22]	Windows 95/98/ME/ NT 4.0/2000	Windows ME, 98se, 98, 95, 2000, NT 4.0	A vulnerability exists because Microsoft Data Access Component Internet Publishing Provider fails to properly determine the origin of WebDAV requests that could let a remote malicious user gain access to sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-022.asp	Windows WebDAV Scripted Request	Medium	Bug discussed in newsgroups and websites.
Microsoft[23]	Windows 95/98/NT 4.0/2000	Internet Explorer 5.5, Windows 98, 2000	A vulnerability exists by double clicking from Window Explorer or Internet Explorer on filenames, which could let a malicious user execute arbitrary programs.	Workaround (Georgi Guninski): Do not double-click from Windows Explorer or Internet Explorer	Windows Explorer and Internet Explorer CLSID File Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[24]	Unix	Darren Reed IPFilter 3.3.1-3.3.10, 3.2.1-3.2.22, 3.3.1-3.3.22, 3.4.1-3.4.17; FreeBSD 2.2.2-2.2.8, 3.0-3.5.1, 4.0-4.2; NetBSD 1.2.1, 1.3-1.3.3, 1.4-1.4.3, 1.5; OpenBSD 2.3-2.8	A vulnerability exists in the fragment handling code, which could allow a malicious user to obtain access to any other UDP or TCP port on the same host.	**Darren Reed:** ftp://coombs.anu.edu.au/pub/net/ip-filter/ip-fil3.4.17.tar.gz **FreeBSD:** ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-01:33/ipfilter.patch	IPFilter Fragment Rule Bypass	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[21] Microsoft Security Bulletin, MS01-021, April 16, 2001.
[22] Microsoft Security Bulletin, MS01-022, April 19, 2001.
[23] Georgi Guninski Security Advisory 42, April 16, 2001.
[24] Securiteam, April 9, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

Multiple Vendors[25]	Unix	HP-UX 10., 10.10, 10.20, 10.30, 11.0;
		FreeBSD 2.x,, 3.x, 4.x;
		OpenBSD 2.3-2.8;
		NetBSD 1.2.1, 1.3-1.3.3, 1.4-1.4.3, 1.5;
		IRIX 6.5.x;
		Solaris 2.3, 2.4, 2.5, 2.5.1, 2.6, 7.0, 8.0
			Multiple FTP server implementations contain buffer overflows that are related to the use of the glob() function, which could allow local and remote malicious users to gain root privileges.	**Workaround:**
				Ensure that no directories exist in the anonymous FTP tree that is writable by the anonymous FTP user. BSD and Irix users should take care to ensure that no directory in the anonymous FTP tree has a name longer than 8 characters. NOTE: These precautions will not prevent local user privilege escalation through the FTP daemon.
				OpenBSD:
				ftp://ftp.openbsd.org/pub/OpenBSD/patches/2.8/common/025_glob.patch
				For more information and patch availability, please read CERT Advisory CA-2001-07 available at:
				http://www.cert.org/advisories/CA-2001-07.html
					Multiple ftpd glob() Buffer Overflow Vulnerabilities
					CVE Name: CAN-2001-0247, CAN-2001-0248, CAN-2001-0249
						High	Bug discussed in newsgroups and websites.
							Vulnerability has appeared in the Press and other public media.

Multiple Vendors[26]	Unix	Linux kernel 2.4, 2.4.0-test1, 2.4.1, 2.4.2, 2.4.3	A vulnerability exists when IPTables are used to allow ftp “RELATED” connections through the firewall which could let a malicious user open arbitrary holes in the firewall and insert entries into the Firewall's RELATED rule set table allowing the FTP Server to connect to any host and port protected by the Firewall's rules.	**NetFilter:** http://netfilter.samba.org/security-fix/	IPTables FTP Stateful Inspection Arbitrary Filter Rule Insertion	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[25] Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2001-02, April 9, 2001.
[26] Securiteam, April 17, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[27]	Unix	Samba 2.0.4- 2.0.7	A vulnerability exists due to the insecure creation of files in the /tmp file system, which could let a malicious user alter contents of other files on the system, and potentially gain superuser privileges.	Upgrade available at: **Samba**: ftp://ftp.samba.org/pub/samba/samba-2.0.8.tar.gz **Debian:** http://security.debian.org/dists/stable/updates/main/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **MandrakeSoft:** ftp://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/updates/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/ **Caldera:** ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/ **Immunix:** http://immunix.org/ImmunixOS/6.2/updates/RPMS/	Samba Insecure TMP file Symbolic Link	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[28]	Unix	ISC INN 2.0- 2.2.3	A buffer overflow vulnerability exists due to insufficient bounds checking in the innfeed program, which could let a malicious user execute arbitrary commands.	**ISC:** ftp://ftp.isc.org/isc/inn/inn-2.3.1.tar.gz	Innfeed Command-Line Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[29, 30]	Unix	Infodrom cfingerd 1.4.0-1.4.3; Debian Linux 2.2, 2.2rl, 2.2r2	A format string vulnerability exists in the logging facility, which could let a remote malicious user gain root privileges and execute arbitrary code.	**Infodrom:** http://www.infodrom.ffis.de/projects/cfingerd/download/cfingerd-1.4.3.tar.gz **Debian:** http://security.debian.org/dists/stable/updates/main/	Cfingerd Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
NCM[31]	Multiple	Content Management System	Due to improper checking, a vulnerability exists in the content.pl script, which could let a malicious user execute arbitrary SQL queries.	Upgrade available at: http://www.thinkthewebway.com/en/services/hotline/responder.pl	Content Management System content.pl Input Validation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape[32]	Windows 95/98/NT 4.0/2000, Unix	Netscape Smart Download 1.3	A buffer overflow vulnerability exists in the 'sdph20.dll' library, which could let a malicious user execute arbitrary code or gain administrative privileges.	Upgrade available at: http://home.netscape.com/download/smartdownload.html	Smart Download Buffer Overflow CVE Name: CAN-2001-0262	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[27] SecurityFocus, April 20, 2001.
[28] Defcom Labs Advisory, def-2001-19, April 18, 2001.
[29] Bugtraq, April 11, 2001.
[30] Debian Security Advisory DSA-048-1, April 18, 2001.
[31] Securiteam, April 16, 2001.
[32] @stake Security Advisory, A041301-1, April 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Nobreak Technologies[33]	Multiple	CrazyWWW Board version 2000p4, 2000LEp5	A buffer overflow vulnerability exists which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CrazyWWW Board Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Oracle Corporation[34]	Multiple	Oracle8 8.0x	A Denial of Service vulnerability exists in the 'TNSLSNR80.EXE' process.	No workaround or patch available at time of publishing.	Oracle 8 Server 'TNSLSNR80. EXE' Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Oracle Corporation[35]	Unix	Application Server 4.0.82	A buffer overflow vulnerability exists in the shared library 'ndwfn4.so' that could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Oracle Application Server ndwfn4.so buffer overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
PGP Security, Inc.[36]	Windows 95/98/ME/ NT 4.0/2000	PGP for Personal Privacy/PGP Desktop Security/ PGPfreeware 5.0 - 7.0.4 (Windows)	A vulnerability exists in the PGP ASCII Armor parser, which could let a malicious user execute arbitrary code.	Patch available at: http://download.nai.com/products/licensed/pgp/desktop_security/windows/version_7.04/hotfix/PGPDS704Hotfix1.zip	PGP (Pretty Good Privacy) ASCII Armor Parser Vulnerability	**High**	Bug discussed in newsgroups and websites.
QPC Software[37]	Windows 95/98/NT 3.5.1/4.0/ 2000	QVT/Term Plus 5.0, QVT/Net 5.0	A directory traversal vulnerability exists which could let a malicious user gain sensitive information and an unchecked buffer in the login function can cause a Denial of Service.	No workaround or patch available at time of publishing.	QVT Suite FTP Server Directory Traversal and Buffer Overflow	Low/ Medium	Bug discussed in newsgroups and websites.
Qualcomm[38]	Windows 95/98/NT 4.0/2000	Eudora 5.0.2, 5.1	A vulnerability exists which could let a malicious user get any file from a users hard drive if he can make the receiving party forward a mail containing a false attachment reference to this local file.	No workaround or patch available at time of publishing.	Eudora File Attachment	Medium	Bug discussed in newsgroups and websites.
RobTex[39]	Windows 95/98/NT 3.5.1/4.0/2000	Viking Server 1.0.5-1.0.7-369	A directory traversal vulnerability exists which could let a malicious user gain sensitive information.	Upgrade available at: http://www.robtex.com/viking/	Viking Server Hex Encoded Directory Traversal	Medium	Bug discussed in newsgroups and websites.

[33] Securiteam, April 11, 2001.
[34] Bugtraq, April 18, 2001.
[35] S.A.F.E.R. Security Bulletin 0016, April 10, 2001.
[36] @stake Security Advisory, A040901-1, April 20, 2001.
[37] Strumpf Noir Society Advisories, April 13, 2001.
[38] Bugtraq, April 18, 2001.
[39] Bugtraq, April 17, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SCO[40] ***Patch now available[41]***	**Unix**	**OpenServer 5.0 -5.0.6**	**Buffer overflow vulnerabilities exist in the lpusers application, lpshut application, recon application, lpforms application, lpadmin application, deliver application, and the sendmail application which could allow a malicious user to elevate their privileges.**	***Patch available at:*** ftp://ftp.sco.com/SSE/sse072b.tar.Z	**Multiple SCO Buffer Overflow Vulnerabilities**	**Medium**	**Bug discussed in newsgroups and websites.**
Sun Micro-Systems[42]	Unix	Solaris 2.6	A buffer overflow vulnerability exists in glob()recover which could let a malicious user recover parts of the shadow file containing encrypted passwords. This could lead to elevated privileges.	No workaround or patch available at time of publishing.	Solaris FTP Core Dump Shadow Password Recovery	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Micro-systems, Inc.[43]	Unix	Solaris 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the kcms_configure (Kodak Color Management System) utility that could let a malicious user gain root privileges.	No workaround or patch available at time of publishing.	Solaris kcms_ configure Command-Line Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Micro-systems, Inc.[44]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the environment variable handled by the kcsSUNWIOsolf.so library which could let a malicious user compromise root.	No workaround or patch available at time of publishing.	Solaris kcms_ configure KCMS_ PROFILES Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Sun Micro-systems, Inc.[45]	Unix	Solaris 2.3, 2.4, 2.5, 2.5.1, 2.6, 7.0, 8.0	A buffer overflow vulnerability exists in the HOME environment variable, which could let a malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	Solaris Xsun HOME Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Micro-systems, Inc.[46]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the CDE Session Manager 'dtsession' which could let a malicious user gain root privileges.	No workaround or patch available at time of publishing.	Solaris CDE dtsession Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Micro-systems, Inc.[47]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86	A vulnerability exists in the ftp daemon, which could let a malicious user gain access to names of valid user accounts.	No workaround or patch available at time of publishing.	Solaris IN.FTPD CWD Username Enumeration	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[40] Reconnaissance Team Security Advisories, SRT2001-02 through SRT2001-07, March 27, 2001.
[41] System Security Enhancement (SSE) SSE072B, April 12, 2001.
[42] Bugtraq, April 19, 2001.
[43] eSecurityOnline Free Vulnerability Alert 3543, April 10, 2001.
[44] Bugtraq, April 11, 2001.
[45] eEye Digital Security, April 10, 2001.
[46] Bugtraq, April 11, 2001.
[47] Bugtraq, April 11, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[48]	Unix	Sun Solaris 7.0_x86	A buffer overflow vulnerability exits in the /usr/bin/i86/ipcs utility which could let a malicious user execute arbitrary code and potentially gain elevated privileges.	A temporary workaround is to remove the SGID bit from ipcs	Solaris IPCS Timezone Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
SuSE[49]	Unix	Linux 7.0, alpha, ppc, sparc	A vulnerability exists because KFM insecurely creates a directory to store its cache contents, which could let a malicious user overwrite and corrupt files.	No workaround or patch available at time of publishing.	KFM Insecure TMP File Creation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SuSE[50]	Unix	NEdit 5.5.1	A vulnerability exists in the Nirvana Editor (Nedit), which could let a malicious user gain elevated privileges, possibly root.	Update available at: ftp://ftp.suse.com/pub/suse/i386/update/	NEdit Temporary File Creation	Medium/ **High**	Bug discussed in newsgroups and websites.
Sybase & Symantec[51]	Windows 98/NT 4.0/2000	Adaptive Server Anywhere Database Engine 6.0.3.2747, Symantec Ghost 6.5	A buffer overflow vulnerability exists in the Sybase Adaptive Server Anywhere Database Engine that is shipped with Symantec Ghost which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Upgrade available at: http://www.symantec.com/ghost	Sybase Adaptive Server Anywhere Database Engine Buffer Overflow And Symantec Ghost Configuration Server Denial of Service	Low/**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Timecop[52]	Unix	BubbleMon up to 1.32 (FreeBSD)	A vulnerability exists in the bubblemonapp, which could let a malicious user execute arbitrary commands.	Upgrade available at: http://www.ne.jp/asahi/linux/timecop/software/bubblemon-dockapp-1.32.tar.gz	BubbleMon Privilege Elevation	**High**	Bug discussed in newsgroups and websites.
Trend Micro[53]	Unix	Interscan Viruswall (Linux) 3.0.1	Several buffer overflow vulnerabilities exists in the ISADMIN service, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://www.trend.com/support	Interscan Viruswall Multiple Program Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Watch Guard[54]	Unix	FireboxII Firmware 4.1-4.5	A remote Denial of Service vulnerability exists when a malicious user sends a custom crafted burst of packets.	Upgrade available at: http://www.watchguard.com/support	Firebox II Malformed Packet Rate Denial of Service	Low	Bug discussed in newsgroups and websites.

[48] Bugtraq, April 12, 2001.
[49] Bugtraq, April 18, 2001.
[50] SuSE Security Announcement, SuSE-SA:2001:14, April 19, 2001.
[51] Defcom Labs Advisory def-2001-21, April 11, 2001.
[52] Bugtraq, April 16, 2001.
[53] eEye Digital Security, April 13, 2001.
[54] Defcom Labs Advisory, def-2001-18, April 5, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Way to the Web Limited[55]	Windows NT 4.0, Unix	TalkBack 1.1	A directory traversal vulnerability exists in the Talkback.cgi, which may allow a remote malicious user to gain sensitive information.	Update available at: http://www.waytotheweb.com /webscripts/talkback.htm	TalkBack.cgi Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Zetetic Enterprises [56]	Palm OS	Strip 0.3, 0.4, 0.5	Strip (Secure Tool for Recalling Important Passwords) contains a vulnerability in the SysRandom() syscall that could let a malicious user obtain the encrypted password.	A workaround is to change all passwords that were generated via Strip using system utilities.	Strip Password Generator Limited Password-Space	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system and/or the intruder can execute or alter arbitrary system files. An example of this would be a vulnerability, in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 20, and April 8, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 38 scripts, programs, and net-news messages containing holes or exploits were identified.
NOTE: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
April 20, 2001	Fk-0014.zip	Forbidden Knowledge Issue 14 has techniques for reconstructing serialized Java objects from sniffer logs, Blackhole TCP/UDP behavior and its effect of nmap.
April 20, 2001	**Iexslt.txt**	**Demonstration exploit for the MS Windows Explorer and Internet Explorer CLSID File Execution vulnerability.**
April 20, 2001	Webspider_1.1.pl	A Perl script that, when given a start page, will "follow" every link it finds, scanning the HTML code for the use of CGI's.

[55] Whizkunde Security Advisory, April 9, 2001.
[56] Securiteam, April 12, 2001.

Date of Script (Reverse Chronological Order)	**Script Name**	**Script Description**
April 19, 2001	Xlock.txt	Technique for removing the SUID bit from xlock which causes enter to work as a password to unlock the screen for all users except root.
April 18, 2001	**Kick_orcl.pl.b64**	**Script which exploits the Oracle 8 Server 'TNSLSNR80.EXE' Denial of Service vulnerability.**
April 18, 2001	X-innfeed.sh	Script which exploits the innfeed Command-Line Buffer Overflow vulnerability.
April 18, 2001	X-startinnfeed.c	Script which exploits the innfeed Command-Line Buffer Overflow vulnerability.
April 17, 2001	Brute.sh	Script which exploits the CrossWind CyberScheduler 'websyncd' remote Buffer Overflow vulnerability.
April 17, 2001	Nf-drill.pl	Perl script which exploits the IPTables FTP Stateful Inspection Arbitrary Filter Rule Insertion vulnerability.
April 17, 2001	X-cybershcehd.c	Script which exploits the CrossWind CyberScheduler 'websyncd' remote Buffer Overflow vulnerability.
April 16, 2001	Clsidext.txt	Technique for exploiting the Window Explorer or Internet Explorer filename extensions vulnerability.
April 16, 2001	Crank-0.1.1.tar.gz	A plug-in architecture that includes automatic and manual monoalphabetic crackers, an n-gram statistics display, a set of simple text filters, and a notepad.
April 16, 2001	Fbsdftp-ex.c	Script which exploits the FreeBSD v4.2 ftpd GLOB vulnerability.
April 16, 2001	Globulka.pl	Perl script which exploits the FreeBSD-4.2-Stable ftpd GLOB vulnerability.
April 16, 2001	**ISA.dos.txt**	**Exploit URL for the Denial of Service vulnerability in Microsoft ISA server v1.0.**
April 16, 2001	Msp-0.01.tar.gz	A commandline tool that allows you to construct buffer overflow strings.
April 16, 2001	Openbsd.glob.c	Script which exploits the OpenBSD 2.x ftpd GLOB vulnerability.
April 16, 2001	Repeat.c	Script which exploits the Internet & Acceleration Server Denial of Service vulnerability.
April 16, 2001	Shijack.tgz	A TCP connection hijacking tool for Linux, FreeBSD, and Solaris.
April 16, 2001	Spapem.tar.gz	The Spapem project shows how to elude securelevel under *BSD systems by hiding the fact that the system has been rebooted.
April 16, 2001	**Testhta1.zip**	**Demonstration exploit for the MS Windows Explorer and Internet Explorer CLSID File Execution vulnerability.**
April 14, 2001	Ethereal-0.8.17-a.tar.gz	A GTK+-based network protocol analyzer that lets you capture and interactively browse the contents of network frames.
April 13, 2001	Sdsploit.tar.gz	Script that exploits the Netscape Smart Download 1.3 Buffer Overflow vulnerability.
April 12, 2001	Lc3setup.exe	An NT password auditing tool which will compute NT user passwords from the cryptographic hashes that are stored by the NT operation system.
April 12, 2001	Strip-crack.c	Script which exploits the Strip Password Generator Limited Password-Space vulnerability.
April 11, 2001	Fingex.pl	Perl script which exploits the cfingerd Format String vulnerability.
April 11, 2001	**Solsparc_kcssunwiosolf.c**	**Script which exploits the Solaris kcms_ configure KCMS_ PROFILES Buffer Overflow vulnerably.**
April 11, 2001	**Solx86_dtsession.c**	**Script which exploits the CDE dtsession Buffer Overflow vulnerability.**
April 11, 2001	**Solx86_kcssunwiosolf.c**	**Script which exploits the Solaris kcms_ configure KCMS_ PROFILES Buffer Overflow vulnerably.**

Date of Script (Reverse Chronological Order)	Script Name	Script Description
April 10, 2001	**Crazywwwb-exploit.pl**	**Perl script which exploits the CrazyWWWBoard Remote Buffer Overflow vulnerability.**
April 10, 2001	Ipfilter-exp.txt	Technique for exploiting the IPFilter Fragment Rule Bypass vulnerability.
April 10, 2001	**Kcms_configure_overflow.c**	**Script that exploits the Solaris kcms_ configure Command-Line Buffer Overflow vulnerability.**
April 10, 2001	**Nphmailex.pl**	**Perl script which exploits the nph-maillist Arbitrary Code Execution vulnerability.**
April 10, 2001	**Xsunexp.c**	**Script which exploits the Solaris Xsun HOME Buffer Overflow vulnerability.**
April 9, 2001	Ettercap-0.4.0.tar.gz	A network sniffer/interceptor/logger for switched LANs, which uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
April 9, 2001	Talkback.txt	Exploit URL for the Talkback.cgi vulnerability.
April 8, 2001	Arpinject.zip	Windows tool which sends custom ARP reply packets at a specified interval, causing most systems to update their ARP tables.
April 8, 2001	Kmailbug.c	Script which exploits the Kmail Remote Buffer Overflow vulnerability.

Trends

Probes/Scans:

There has been an increase in the number of scans and attacks to port 515 looking for the LPRng User-Supplied Format String vulnerability, Wu-Ftpd Remote Format String Stack Overwrite Vulnerability, ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability, and the rpc.statd Remote Format String Vulnerability.

There has been an increase in the number of suspicious probes and scans designed to find vulnerable domain name servers on corporate networks.

Other:

NIPC has issued an advisory concerning a potential security vulnerability that exists in PDG Software, Inc. Shopping Cart software (versions prior to 1.63) which is being actively exploited. For more information, please see NIPC ADVISORY 01-007, located at: http://www.nipc.gov/warnings/advisories/2001/01-007.htm.

Numerous reports have been received indicating that the snmpXdmid vulnerability is actively being exploited which could allow a malicious user to gain root access. For more information, please see CERT® Advisory CA-2001-05, located at: http://www.cert.org/advisories/CA-2001-05.html.

Worms are being released based on well-known exploits such as Bind, LPRng, rpc-statd, and wu-ftpd.

A software package has been released which, if used maliciously, may disable a victim's computer or network's IDS by flooding it with Internet traffic emanating from several random Internet Protocol (IP) addresses simultaneously. For more information, please see NIPC ASSESSMENT 01-004, located at: http://www.nipc.gov/warnings/assessments/2001/01-004.htm.

Viruses

A list of viruses infecting two or more sites as reported to various anti-virus vendors and virus incident reporting organizations has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table list the viruses by: ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. These types of malicious code will also now be included in the table. Following this table are write-ups of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **222** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **440** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Hybris	Worm	Stable	November 2000
2	PE_MTX.A	File Infector, Trojan	Slight increase	September 2000
3	VBS/Kakworm	Script	Slight decrease	December 1999
4	VBS/Loveletter	Script	Slight increase	March 2000
5	W32/Navidad	File, Worm	Slight decrease	November 2000
6	W32/Magistr	File, Worm	New to table	March 2001
7	VBS/SST	Script, Worm	Slight decrease	February 2001
8	W32/Bymer	Worm	Return to table	October 2000
9	W32/Funlove	File	Slight decrease	November 1999
10	W97M/Marker	Macro	Return to table	August 1998

ELF_ADORE.A (Aliases: Unix/Adore, ADORE.A, Red Worm, Linux/Adore): This Internet Worm is similar to ELF_RAMEN and ELF_LION.A that infects Linux Operating Systems. The Adore worm utilizes known vulnerabilities of Linux systems, such as BIND, wu-ftpd, rpc-statd, and lpd services to infect. Once the system is infected, the worm package is downloaded and the worm is executed. After this the worm establishes a backdoor component. The worm is capable of deleting all traces of itself except the backdoor component.

JS.Congrats.A@mm (JScript E-mail Worm): The worm arrives as an attachment named Original.jpg. When executed, the worm e-mails itself to everyone in the contact list of your Microsoft Outlook address book. When run, JS.Congrats.A@mm recursively deletes all .jpg files found on the drive C, with the exception of those in the root directory.

IRC_LOGOLOGIC.A (Aliases: LOGOLOGIC.A, I-Worm.LogoLogic.A Logic (IRC Script Worm): This worm is the first malicious code written in the Logo programming language that is currently being used for educational purposes only at a limited number of schools. "Logic" has the capacity to spread via e-mail utilizing the widely available Microsoft Outlook mail program as well as IRC (Internet Relay Chat) channels. Apart from unauthorized spreading, the Internet-worm has no additional payload that would affect the normal operating procedures of the infected computers. The message "Logic" distributes to all recipients from the Outlook address book appear as follows:

Hello! Look at my new SuperLogo programme! Isn't it cool?

JS.Optiz (JScript E-mail Worm): When executed, the script infects the files that have the .js extension (JScript script files) that it finds in the current folder (the folder from which the script runs) and in the \Windows folder. If the Windows version is Windows 95, 98, or ME, it also infects JScript files found in the \Desktop folder.

VBS_LOVELETTR.CX (Aliases: LOVELETTR.CX, I-Worm.Loveletter, VBS/Gorum, VBS.Chunxiao@mm) (Visual Basic Script Worm): This Visual Basic script virus is a variant of the VBS_LOVELTTER worm. It uses Microsoft Outlook to send itself to all entries listed in the address book of the infected user. Upon execution, this worm creates three copies of itself, NAVAPW32.VBS and XIAOCHUN.TXT.VBS in the Windows System folder, and PCCNT.VBS in the Windows folder. Then it adds the following two registry entries so that the worm is loaded at every Windows start up:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
"Norton Auto-Protect = \Navapw32.vbs"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\
"Trend OfficeScan = \Pccnt.vbs"

The subject and the message body of this e-mail are Chinese characters.

VBS.PassOn (Visual Basic Script Worm): This virus is stored as either a vbs file or an .html file. When VBS.PassOn is executed, it changes the default home page of Microsoft Internet Explorer by creating the value:

http://www.passthison.com

in the following registry key:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page

VBS.Pie@mm (Alias: VBS.Pie) (Visual Basic Script Worm): This worm spreads by sending itself to all addresses in the Microsoft Outlook address book. It also spreads by mIRC. The worm arrives with an attachment named Su_Premio.txt.vbs and is very similar to the VBS.Plan worm.

VBS.Voodoo.A (Alias: VBS/Voodoo.2312) (Visual Basic Script Worm): This worm infects files with the .html, .htm, and .htt (html template) file extensions. When you open an infected file, VBS.Voodoo.A changes the Value data of the following registry keys to 0 (zero):

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1201
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1201

This reduces the security protection that is provided by Microsoft Internet Explorer. By inserting virus code into .htt files, the virus is executed every time that you click in the left pane of Windows Explorer. The virus also changes the .html file icon to the Recycle Bin icon.

VBS.Zeta.A@mm (Visual Basic Script Worm): This is a worm, which uses Microsoft Outlook and mIRC to spread itself. It overwrites .vbs and .vbe files with a copy of the worm. When the worm is executed, it does the following:

- Copies itself to the \Windows\System folder as FotoPorno2.jpg.vbs.
- Searches for the mIRC program folder. If present, the worm overwrites the Script.ini file to spread itself when connected to mIRC.
- Sends an e-mail message to all contacts on all address lists found in Microsoft Outlook.
- Searches for .vbs and .vbe files on all mapped drives, shared drives, and hard drives. It overwrites these files with a copy of itself.

- Adds the following value:
  ZetaBait wscript.exe <Windows System Folder>\FotoPorno2.jpg.vbs %
  to the following registry key:
  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  to enable itself to run at startup.

W32/Badtrans-A (W32 Worm): This is a worm that uses MAPI to spread. The worm arrives in an e-mail message with the text "Take a look to the attachment." If the attached file is run, it displays the message "File data corrupt probably due to bad data transmission or bad disk access," and copies itself into the Windows directory with the filename INETD.EXE. It also changes win.ini so that the file is run at Windows startup. When a new message arrives, the worm sends a reply with an infected attachment. The worm also drops a file kern32.exe, which is a password-stealing Trojan, Troj/Keylog-C (See Trojan Section), into the Windows system directory and changes the registry key \HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce so that the Trojan runs at the startup of Windows.

W32.Lastword@mm (W32 Worm): This worm sends a copy of itself to all entries in all Microsoft Outlook address lists, and adds a copy of itself in the root directory of every hard drive. If an infected computer is restarted three times, then the worm will delete C:\Windows\System.ini. When the worm is first executed, it copies itself to C:\Windows using one of these file names:

Posta_Update.exe
Win_Update.exe
Win32_Update.exe
BiHNet.exe

W32/Matcher (W32 Worm): This worm has been reported in the wild. It is a mass-mailing worm that arrives as an e-mail with the following characteristics:

Subject line: Matcher
Message text: Want to find your love mates!!! Try this its cool... Looks and Attitude Matching to opposite sex.

Attached filename: matcher.exe. If the attached file is opened it copies itself into the Windows system and temp directories, changing the system registry entry HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ to point to the file in the system directory. The worm will start continuously sending itself using addresses from the Outlook address book. The worm also makes changes to the existing AUTOEXEC.BAT file on the C: drive, appending the lines:

```
@echo off
echo from: Bugger
pause
```

W97M.Bobo.F.Gen (Word 97 Macro Virus): This virus is similar to many other Microsoft Word macro viruses. When run, it disables the warning message that appears by default when you open a document that contains a macro. This macro virus does not have a malicious payload.

W95.Blakan.2016 (Word 95 Macro Virus): This virus infects .exe files on all local hard drives and network drives. When a file that is infected, the virus will search for .exe files on all hard drives and network drives from C to Z. A file is infected if:

- It contains two sections where the end of the one section and the start of the next section are large enough to hold the virus body and decryptor.
- It contains a writable section that is large enough to hold the decrypted body.
- It contains a call to the ExitProcess() funct ion.

If these criteria are met, then the virus hooks the ExitProcess() function and places itself at the original end of the section that will contain it, and shifts the remaining contents of the file.

W97M.Sacep.A (Word 97 Macro Virus): This is a simple macro virus that adds the text:

pequitas te amo

to infected documents on the 13th of every month. It spreads when you close an infected document.

WM97/Buendia-B (Word 97 Macro Virus): On the 28th of any month this virus will display the message "HOY ES UN BUEN DIA," wait for 1 minute and then display the message "LUCY POR SIEMPRE TE RECORDARE atte: JAIRO."

WM97/Goober-E (Word 97 Macro Virus): This virus is a member of the WM97/Goober family. The virus searches through documents and replaces any occurrence of "ShiThe!" or "shithe" with "The" and "the" respectively. It also creates the non-viral text file C:\G00ber.sys, which it uses during replication.

WM97/Marker-GZ (Word 97 Macro Virus): This virus has been reported in the wild. It keeps a log file of infections, and may create the non-viral file C:\pagefile.log.

WM97/Thus-DB (Word 97 Macro Virus): This virus is a member of the WM97/Thus family of Word macro viruses, but the payload has been removed.

X97M.Adn.C.Gen (Aliases: X97M.Adn.A, X97M.Adn.B, Macro.Excel97.And) (Excel 97 Macro Virus): This virus infects the active Microsoft Excel workbook, and infects the system by inserting an infected workbook in the Office folder. When run on a computer for the first time, X97M.Adn.C.Gen checks to see if the system is already infected. If it is not, the infected workbook is inserted as \Office\Personal.xla. This file is saved as an Add-In. On infecting other workbooks, the macro name is randomly created. The name consists of a letter followed by a number ranging from 1 to 1000. Every time that X97M.Adn.C.Gen is activated, it generates a random number between 1 and 31. If this number matches the current day of the month, the payload is executed. The payload performs two actions:

It changes the window title to "Spalaci.Label.Is.Pac"

It changes the tool bar buttons from small buttons to large ones.

X97M.Hihihoho (Excel 97 Macro Virus): This virus infects Microsoft Excel worksheets. The virus does not attempt to stealth itself in any way, so when an infected worksheet is opened in Excel 97 or Excel 2000, the Microsoft macro virus warning dialog box should appear. The virus spreads its infection by copying itself to other Microsoft Excel worksheets that are opened while an infected worksheet is open. The virus prevents multiple infections by checking for the comment "Hihihihohoho" prior to infecting a worksheet.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.WLF	**N/A**	**Current Issue**
Backdoor-JZ	N/A	CyberNotes-2001-02
BAT.Install.Trojan	N/A	CyberNotes-2001-04
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07

Trojan	Version	CyberNotes Issue #
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
Flor	N/A	CyberNotes-2001-02
HardLock.618	N/A	CyberNotes-2001-04
JS.StartPage	N/A	CyberNotes-2001-07
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog -C	**N/A**	**Current Issue**
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	**N/A**	**Current Issue**
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_EUTH.152	**N/A**	**Current Issue**
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IE_XPLOIT.A	**N/A**	**Current Issue**
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_JOINER.I	**N/A**	**Current Issue**
TROJ_MATCHER.A	**N/A**	**Current Issue**
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNot es-2001-03
TROJ_SCOUT.A	**N/A**	**Current Issue**
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03

Trojan	Version	CyberNotes Issue #
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	**N/A**	**Current Issue**
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
VBS.Zeichen.A	**N/A**	**Current Issue**
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07

Backdoor.WLF: This Trojan is a backdoor program that works similarly to Backdoor.NTHack. It is normally installed remotely by another user. It also utilizes a UPX packed version of the legitimate WinGate application to do its job. Once Backdoor.WLF is installed, it allows other users to access the Internet through the victimized computer. The victimized computer may then start acting like a proxy server. A possible malicious application of this feature is for remote user to perform unauthorized downloads on this victimized computer, making it look legitimate, since it would be requested by an acting proxy server.

TROJ_BADTRANS.A (Aliases: BADTRANS.A, W32.Badtrans.13312@mm, I-WORM.BADTRANS): This memory resident Internet worm propagates via e-mail clients that use Windows sockets, such as Microsoft Outlook and Outlook Express. It replies to all unread e-mail messages with itself attached to the e-mail. The e-mail sent by the worm has the same subject header and message body as the original e-mail. The name of the sender will be the name of the user who is currently logged on to the infected computer. This worm also modifies WIN.INI so that it is executed at the next re-boot.

TROJ_EUTH.152 (Aliases: Euthanasia 1.52, Spam/Euthanasia.152, Spammer. Euthanasia.152): This Trojan is an e-mail message tool that was created with Borland Delphi 4.0. It is designed to create and send forged e-mail messages to any intended recipient. The sender only needs to specify the e-mail server to use and the e-mail address of the intended recipient. The sender may also choose a bogus X-mailer header to authenticate the forged e-mail. The X-mailer header refers to the e-mail client that the message was supposedly created by. Files can also be attached to the e-mail message.

TROJ_IE_XPLOIT.A (Alias: IE_XPLOIT.A): This EXE file, programmed in Visual Basic 5, is embedded in an EML (MS Outlook Express message file format). EML files are MIME multipart files that Internet Explorer 5 parses. A vulnerability exists that allows arbitrary code execution when these files are used. The vulnerability allows a hostile page or e-mail to perform any action on an infected computer. Upon opening the EML file with embedded EXE codes of this Trojan, the following message is displayed in a message box with an OK button:

Title: Project1
Message Body: I have written a file: C:\WINDOWS\TEMP\deleteme.txt

When the OK button is clicked, it attempts to drop its displayed file, DELETEME.TXT that does not contain any malicious code. Thereafter, it displays another message box with the following message:

Title: Security Issue
Message Body: Your system has a vulnerability

TROJ_JOINER.I (Aliases: Multidropper.m, TROJ_JOINER-I, JOINER.I): This Trojan drops files that function as joiners or binders that combine to run a Trojan and a program in an infected system. This is a variant of the Trojan family Joiner. It carries no destructive payload.

Troj/Keylog-C: This Trojan is dropped by the W32/Badtrans-A worm. When the Trojan runs, it attempts to send user-confidential information such as passwords, operating system details and keyboard keys pressed to an attacker.

TROJ_MATCHER.A (Aliases: Matcher.A, Lonely Hearts Virus): This Trojan comes disguised as a Love Matching program. It was created in Visual Basic 6.0 and uses the Visual Basic component Microsoft Script Control to propagate using Microsoft Outlook. It tries to send an e-mail with itself as an attachment twice to all addresses listed in the infected user's address book. This e-mail contains the subject "Matcher" and the attachment "MATCHER.EXE." After the second e-mail is sent, an error message is displayed.

TROJ_SCOUT.A (Aliases: Trojan.PSW.Hooker.B, SCOUT.A): This password-stealing Trojan installs itself in Windows and then stays in memory as a hidden process. It collects sensitive information such as the Windows password and network password and sends them to an e-mail address known to its author, via SMTP.

TROJ_WINMITE.10 (Aliases: Backdoor.WindowsMite, BackDoor-EB, Windows Mite Server, WINMITE.10): This memory-resident backdoor Trojan allows a remote malicious user access to an infected system. It appears as a Windows registry checker program, SCANREGW.EXE in an infected system. It compromises network security. Upon execution, the server side of this Trojan overwrites the original Windows registry checker program in the Windows directory, with a copy of itself as SCANREGW.EXE. Since Windows always starts the Windows registry checker, the Trojan file executes at every Windows session. It also creates the following registry keys:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\
DirectOpenGLDirectX=dword:00000000
HKEY_LOCAL_MACHINE\Software\Microsoft\DirectOpenGL\
SettingsAPPID=dword:0000fffa
```

The Trojan then works in the background as a service process that is invisible in the task list. The client side of this Trojan provides a remote hacker with an interface that controls a computer running the server side of this program. A hacker specifies an Internet Protocol address of an infected system and the Transmission Control Protocol (TCP) port where the server operates. By default, the TCP port is 65530.

VBS.Zeichen.A: This is a Trojan horse written in Visual Basic Script (VBS). It pretends to be a script that obtains URLs to sites with porno-related contents. When executed, it appends malicious commands to the C:\Autoexec.bat and shuts down Windows. After the computer is restarted, the commands that were added to the Autoexec.bat file perform a hidden format of drives C and D without prompting and without the ability to unformat. The malicious payload works only under Windows 95, 98, and ME.